U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

January 20, 2022

Mr. Brian M. Boynton
Acting Assistant Attorney General, Civil Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Re: Vulnerability Disclosure Issues in *Curling v. Raffensperger*, No. 17-cv-2989 (N.D. Ga.)

Dear Mr. Boynton:

The Cybersecurity and Infrastructure Security Agency (CISA) respectfully submits this letter in response to the Court's inquiry from the October 7, 2021, and November 19, 2021, hearings in *Curling v. Raffensperger*, No. 17-cv-2989 (N.D. Ga.), at which time the Court offered to receive a letter from CISA regarding our agency's vulnerability disclosure program. This letter provides information about CISA, the importance of vulnerability disclosure programs and processes in general, and CISA's Coordinated Vulnerability Disclosure (CVD) process. The CVD process offers a mechanism for potential vulnerabilities to be shared with the vendor through coordination with CISA. Were the Court to permit the parties to share information on the alleged vulnerability with CISA, CVD is the process CISA would use to receive, assess, and, as needed, coordinate the mitigation of any ongoing risk posed by an identified vulnerability. As explained below, CISA would almost certainly need to disclose the information through the CVD process to the vendor (*i.e.*, Dominion Voting Systems) to analyze and mitigate, if necessary, the alleged vulnerability. Further, if a vulnerability required mitigation, relevant information would need to be shared with affected end users (*e.g.*, users of the ballot marking devices (BMD) system) and the public.

The Cybersecurity and Infrastructure Security Agency

CISA leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. To that end, CISA works with federal, state, local, tribal, and territorial (SLTT), international, and private sector partners to ensure the security and resilience of the nation's critical infrastructure. CISA also serves as the Sector Risk Management Agency (*see* 6 U.S.C. § 665d) for a number of critical infrastructure sectors and subsectors, including the Election Infrastructure subsector of the larger Government Facilities critical infrastructure sector.

CISA has specific statutory authority to receive, analyze, and disseminate information relating to cybersecurity risks and function as a Federal civilian interface for the multi-directional and cross-sector sharing of such information. 6 U.S.C. § 659(c)(9), (5)(A)–(B), (7), (1); *see also* §

659(a)(8) (defining "sharing" as "providing, receiving, and disseminating"). "Cybersecurity risk[s]" include vulnerabilities. 6 U.S.C. § 659(a)(2)(A). Using the cybersecurity risk and vulnerability information it receives and analyzes, CISA is authorized to engage with federal and non-federal entities to provide shared situational awareness and support the mitigation of vulnerabilities across the federal government and non-federal entities. *See* 6 U.S.C. § 659(c)(2). Specific to CISA's mission to coordinate the mitigation of cybersecurity vulnerabilities and risks, CISA has a responsibility to "develop and adhere to Department policies and procedures for coordinating vulnerability disclosures." 6 U.S.C. § 659(n). One such policy and procedure is CISA's CVD process, which CISA makes publicly available at: https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

CISA's Vulnerability Disclosure Process

CISA's CVD process facilitates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with affected vendors. A vulnerability may be identified when an outside entity or person reports having discovered a vulnerability in software or hardware owned, operated, or sold by a vendor or service provider. The goal of CISA's CVD process is for CISA to facilitate an assessment of the potential vulnerability by, at a minimum, the reporter and the affected vendor(s) and/or service provider(s) in a controlled and risk-minimal (*i.e.*, usually confidential) way. Where needed, that assessment may lead to a disclosure of the vulnerability, often paired with an associated software update or mitigation. Through this approach, users and administrators receive clear and actionable information in a timely manner, and risk of harm is minimized.

The CISA CVD process involves five basic steps:

Collection: CISA collects vulnerability reports in three ways: receiving reports of vulnerabilities from security researchers; discovering vulnerabilities through our own staff work; and monitoring public sources of vulnerability information. The first is the primary way that CISA becomes aware of vulnerabilities, with the second and third methods representing much more limited sources for the CISA CVD process. As applicable here, after receiving a report, CISA performs an initial analysis to assess a vulnerability's presence and compares it with existing reports to identify duplicates.

Analysis: CISA alerts the vendor(s) and begins the process of engaging the source of the vulnerability report and vendor together to understand the vulnerability by examining the technical issue(s) and the potential risk the vulnerability represents.

Mitigation Coordination: CISA continues to work with the affected vendor(s) on the development and issuance of patches or updates to mitigate the risk of the vulnerability.

Application of Mitigation: When possible and where necessary, CISA may work with the vendor(s) to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to full public disclosure of the vulnerability.

Disclosure: In coordination with the source of the vulnerability report and the affected vendor(s), CISA strives to ensure accurate and objective disclosures by the vendors, focused on technical remediation and mitigation for asset owners and operators.

Time frames for mitigation development and the type and schedule of disclosure may be affected by various factors. Extenuating circumstances, such as active exploitation of the vulnerability by a malicious cyber actor, threats of an especially serious nature, or situations that require changes to established standards may result in changes to the disclosure timeline. Other factors include, but are not limited to:

- whether the vulnerability has already been publicly disclosed, *i.e.*, published by the source of the vulnerability report;
- potential impact to critical infrastructure, national security, or public health and safety;
- the availability of effective mitigations;
- vendor responsiveness and feasibility of developing an update or patch; and,
- vendor estimate of time required for customers to obtain, test, and apply the patch.

When CISA informs an affected vendor or service provider of a vulnerability, CISA will provide the name and contact information of the vulnerability reporter unless otherwise requested by the vulnerability reporter. As the information-exchange develops, CISA will advise the vulnerability reporter of vendor-reported significant changes in the status of any vulnerability reported, without revealing information provided in confidence by the affected vendor(s) or service provider(s).

Affected vendors will be apprised of any plans to publish information about the vulnerability, and alternate publication schedules may be negotiated with affected vendors, as required.

Throughout this process, CISA carefully stewards the sensitive data involved in these matters, ensuring that CISA shares such information only between the source of the vulnerability report and the vendor until broader disclosure to any additional parties, including customers and ultimately the public, is warranted. As noted above, the ultimate goal is to disclose confirmed vulnerabilities and associated mitigation to the public in a controlled way, so that the entire cyber ecosystem can benefit while minimizing risk of additional harm.

Importance of Vulnerability Disclosure

Vulnerability disclosure is critical to the security of our Nation's information systems. When software vendors become aware of a vulnerability in their product, they can issue an update that removes or mitigates the vulnerability. Malicious cyber actors may independently discover vulnerabilities, so rapid disclosure of vulnerabilities by researchers to software vendors is critical to limiting the window of opportunity for malicious actors to exploit such vulnerabilities. Finally, public disclosure of the vulnerability (usually simultaneous with disclosure of the associated software update or mitigation) protects the wider technology ecosystem.

Concluding Considerations

CISA is prepared to receive potential vulnerability information connected to this litigation, subject to the caveat that CISA would carry out its work as described above, including, as warranted, coordination with the vendor and security researcher as well as broader dissemination of information related to confirmed vulnerabilities to affected end users and the public. It is CISA's understanding that the Court's current orders do not permit the dissemination CISA may

deem necessary and appropriate in order to carry out its mission. It is important to remember that the ultimate goal of vulnerability disclosure is to ensure that researchers and vendors confirm vulnerabilities and produce mitigations, and that the broader community is advised of confirmed vulnerabilities and associated mitigations. CISA could not receive this information from the security researcher if we are unable to carry out our process as described, as this would risk putting CISA in the untenable situation of knowing our stakeholders are subject to a vulnerability that we are unable to effectively work towards mitigating. In the event that the Court modifies its orders to permit disclosure to CISA, CISA requests that such modification explicitly recognize that CISA would be permitted to follow its ordinary operations with respect to effectuating and/or facilitating warranted disclosures. CISA also would not anticipate, by virtue of its CVD engagement, further involvement in the ongoing litigation itself.

Thank you for considering CISA's views on this matter.

Sincerely,

Brandon Wales
Executive Director
CISA